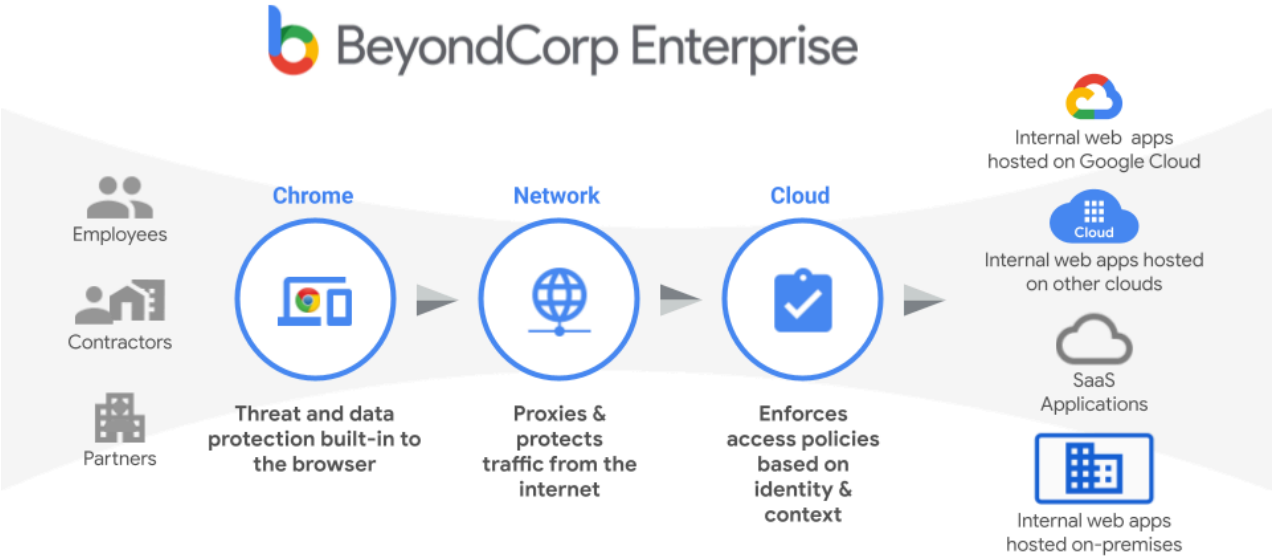
EXHIBIT 5

Chrome Enterprise Premium overview

Today's enterprises are moving to a model of security where secured networks aren't enough. A modern approach is required to truly protect a company's most secure assets and allow for your employees to be productive under the right circumstances.

Chrome Enterprise Premium is Google's tooling meant to empower organizations to enable this new approach. By tying together a user's information with device and location context, an enterprise can make rich access decisions and enforce security policy.



Chrome Enterprise Premium has two key goals:

- Threat and data protection brings security to your enterprise devices by working to protect users from exfiltration risks such as copy and paste, extending DLP protections into the browser, and helping to prevent malware from getting onto enterprise-managed devices.
- Richer access controls protect access to secure systems (applications, virtual machines, APIs, and so on) by using the context of an end-user's request to ensure each request is authenticated, authorized, and as safe as possible.

Bene ts to users

Chrome Enterprise Premium presents a security model that allows for greater security posturing and policy for both applications and devices, while providing end users a better user experience no matter where they access from or what type of device they use to do so:

- For administrators:
  - Strengthen security posture to account for dynamic changes in a user's context.
  - Shrink the access perimeter to only those resources that an end user should be accessing.

- Enforce device security postures for employees, contractors, partners, and customers for access, no matter who manages the devices.
- Extend security standards with per-user session management and multifactor authentication.

- For end users:
  - Allow all end users to be productive everywhere without compromising security.
  - Allow the right level of access to work applications based on their context.
  - Unlock access to personally-owned devices based on granular access policies.
  - Access internal applications without being throttled by segmented networks.

Common use cases

As end users work outside of the office more often and from many different types of devices, enterprises have common security models they are looking to extend to all users, devices, and applications:

- Allow non-employees to access a single web application deployed on Google Cloud or other cloud services platforms without requiring the use of a VPN.
- Allow non-employees to access data from their personal or mobile devices as long as they meet a minimum security posture.
- Ensure employees are prevented from copying and pasting sensitive data into email or saving data into personal storage such as Google Drive.
- Only allow enterprise-managed devices to access certain key systems.
- Provide DLP protections for corporate data.
- Gate access based on a user's location.
- Protect applications in hybrid deployments that use a mix of Google Cloud, other cloud services platforms, or on-premises resources.

Common signals

Chrome Enterprise Premium offers common signals enterprises can take into account when making a policy decision, including:

- User or group information
- Location (IP or geographic region)
- Device
  - Enterprise-managed devices
  - Personally-owned devices
  - Mobile devices
- Third-party device signals from partners in the BeyondCorp Alliance.
  - Check Point

- CrowdStrike
- Lookout
- Tanium
- VMware

Note: Google is not responsible for the accuracy of device data generated by third-party partners. Data provided to Google by the third-party partner is stored as-is. Any inaccuracies or personally identifiable information (PII) reported by the third party partner are the sole responsibility of the partner.

- Risk scores

How to get Chrome Enterprise Premium

Complete this form (https://inthecloud.withgoogle.com/beyondcorp/contact.html) to get more information about upgrading to Chrome Enterprise Premium.

Chrome Enterprise Premium compared with Google Cloud

Chrome Enterprise Premium provides enterprise security features in addition to the basic protections, focused on protecting applications with authentication and authorization, that are baseline features of Google Cloud. Chrome Enterprise Premium extends those protections to applications and data running everywhere, with end-user protections and rich access policy protections.

The following table shows the differences between the baseline features available to Google Cloud customers and what is available with Chrome Enterprise Premium:

Applications and Resources Access	GCP Baseline	BeyondCorp Enterprise Essentials	BeyondCorp Enterprise
Access control to web applications on Google Cloud Platform	✓		✓
Access control to SSH, RDP and TCP ports for VMs on GCP	✓		✓
Access control to Google Cloud Platform APIs	✓		✓
Access control to Google Cloud console	✓		✓
Access control to web applications on GCP internal load balancing	✓		✓
Access control to web applications on customer premises			✓
Access control to thick client / client-server applications			✓
Access control to web applications on AWS and Azure			✓
Access control to SAML-based applications (login time)		✓	✓
Access control to Google Workspace Admin Console		✓	✓
Access Policies and Advanced Settings	**GCP Baseline**	**BeyondCorp Enterprise Essentials**	**BeyondCorp Enterprise**

Access levels using users	✓	✓	✓
Access levels using IP addresses and geolocations	✓	✓	✓
Access levels using time and date restrictions		✓	✓
Access levels using login credential strength		✓	✓
Access levels using enterprise certificates		✓	✓
Access levels using device security postures		✓	✓
Access levels using Chrome security postures		✓	✓
Access levels using third party partner signals		✓	✓
Access levels using advanced expression language		✓	✓
Same-origin policy configuration in HTTP OPTIONS	✓	N/A	✓
Custom authentication domain and 403 pages		N/A	✓
User, Threat, and Data Protection	**GCP Baseline**	**BeyondCorp Enterprise Essentials**	**BeyondCorp Enterprise**
Data loss prevention w/ predefined or custom detectors (Chrome)		✓	✓
Malware protection w/ advanced sandboxing (Chrome)		✓	✓
Phishing and malicious URL protection (Chrome)		✓	✓
Threat and data protection alerting and reporting (Chrome)		✓	✓

What's next

- Learn more about access protection controls (/beyondcorp-enterprise/docs/access-protection)
- Learn more about threat and data protections (https://support.google.com/a/answer/10104463)

Except as otherwise noted, the content of this page is licensed under the Creative Commons Attribution 4.0 License (https://creativecommons.org/licenses/by/4.0/), and code samples are licensed under the Apache 2.0 License (https://www.apache.org/licenses/LICENSE-2.0). For details, see the Google Developers Site Policies (https://developers.google.com/site-policies). Java is a registered trademark of Oracle and/or its affiliates.

Last updated 2025-01-08 UTC.